European Security and Defence College
Doc: ESDC/2022/063
Date: 1 April 2022
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	The Role of the EU Cyber Ecosystem in the Global Cyber Security Stability	ECTS
Feb. 2024	206		1

Target audience

The participants should be mid-ranking to senior officials dealing with aspects in the field of cyber security from EU Member States **and** third states.

Open to:

- EU Member States / EU Institutions Bodies and Agencies
- Third countries
- International Organisations

Aim

This course presents the main pillars of the EU cyber ecosystem and how these pillars can reinforce the global security stability by strengthening the cyber resilience, built trust and upscaling the cooperation among the global actors.

Furthermore, this course will allow the mid-ranking to senior officials to exchange their views and share best practices on cyber-related topics by improving their knowledge, skills and competencies.

By the end of this course the participants will be able to be more interoperable across the global cyber ecosystem and to share some common views.

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber	• *Non-specialised cyber course, at awareness level* • *Linked with the strategic objectives of Pillar 3 of the EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN (2020)]*

Learning Outcomes	
Knowledge	LO1- List the EU policies related to cyber LO2- Identify the entities involved in the EU cyber ecosystem and their respective roles LO3- Define the basic notions and concepts of cybersecurity LO4- Identify the nature of the different cyber threats LO5- Identify the challenges of cyber security at global level LO6- Identify the international cyber space issues and their effect globally LO7- Identify the specific sectors for cooperation globally LO8- Define the basic notions and concepts of hybrid threats

Skills	LO9- Classify the cyber issues according to complexity LO10- Classify the impact of cyber-threats in the global stability LO11- Categorize the cooperation opportunities between the EU cyber ecosystem and the global cyber environment
Responsibility and Autonomy	LO12- Evaluate the potential impacts of cyber threats in the global environment LO13- Create opportunities for synergies between the EU cyber ecosystem and the global cyber environment LO14- Select the appropriate confidence building measures to broaden cooperation in cyberspace

Evaluation and verification of learning outcomes

The course is evaluated according to the Kirkpatrick model: it makes use of *level 1 evaluation* (*based on participants' satisfaction with the course*) and *level 3 evaluation* (*assessment of participants' long-term change in behaviour after the end of the course*). *Evaluation feed-back* is given in the level 1 evaluation on the residential modules.
In order to complete the course, the participants have to accomplish all learning objectives, which are evaluated based on their active contribution to the residential modules, including their syndicate sessions and practical activities as well as on their completion of the eLearning phases: course participants must finalise the autonomous knowledge units (AKUs) and pass the tests (*mandatory*), scoring at least 80% in the incorporated out-test/quiz. **However, no formal verification of the learning outcomes is foreseen; proposed ECTS is based on participants' workload only**.
The Executive Academic Board takes these factors into account when considering the award of *Certificates* to participants. Module leaders provide an evaluation report for each residential module. The Course Director is responsible for overall coordination, with the support of the ESDC Secretariat, and drafts the *final evaluation report* which is presented to the Executive Academic Board.

Course structure

The residential module is held over 3 days.

Main Topic	Suggested Working Hours (required for individual learning)	Suggested Contents
1. The EU Cyber Ecosystem	8 (4)	1. Presentation of EU Agencies and bodies with cyber-related tasks
2. The EU Approach in building resilience in cyberspace	12 (4)	2. Policies - Regulations - Directives related to cyber 2.1. EU Cybersecurity Strategy 2.2. Digital Single Market Strategy for Europe 2.3. Network and Information Security (NIS) Directive 2.4. The Cyber Security Act 2.5. The General Data Protection Regulation 2.6. The EU Coordinated Response to Large Scale Cybersecurity Incidents and Crises 2.1. The Communication of the EU Strategic Approach
3. The EU's External Cyber Capacity Building	5	3. Joint Communication on 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU' 3.1. The EU Cyber Diplomacy Toolbox
4. The EU Approach in Hybrid threats	2	4. The conceptual framework on hybrid threats and the interaction with cyber
TOTAL	**27(8)**	

Material	Methodology
Required: **AKU 2:** European Global Strategy **Recommended:** • *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union* • *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* • *Council conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (November 2016)* • *The EU Cyber Diplomacy Toolbox (June 2017)* • *The EU Cybersecurity Act (June 2019)* • *The EU's Cybersecurity Strategy for the Digital Decade (December 2020)*	The course is based on the following methodology: Presentations, Panels talks, Q&A and/or workshops **Additional information** Pre-course questionnaire on learning expectations and possible briefing topic from the specific area of expertise may be used. All course participants have to prepare for the residential module by going through the relevant eLearning preparatory phase, which is mandatory. The materials proposed for supplemental (eLearning) study will reflect current developments in the field of cyber security/cyber defence in general and EU policies in particular. The Chatham House Rule is applied during all residential phase of the course: "participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed".